REMARKS

These remarks are in response to the non-final Office Action dated August 5, 2005. Claims 1-111 are pending in the application.

In the non-final Office Action, the Examiner rejected claims 1-25, 29-40, 50-62, 64-85, 87-99, 102-103, and 105-111 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,826,694 to Dutta et al ("Dutta"). Claims 26-28, 41-49, 63, 86, 100, and 104 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Dutta in view of U.S. Patent No. 6,598,034 to Kloth ("Kloth").

To clarify the use in the pending claims and to hereby provide notice to the public, the phrase "at least one of <A>, <B>, ... and <N>" is defined by the Applicant in the broadest sense, superseding any other implied definitions herebefore or hereinafter unless expressly asserted by the Applicant to the contrary, to mean one or more elements selected from the group comprising A, B, ... and N, that is to say, any combination of one or more of the elements A, B, ... or N including any one element alone or in combination with one or more of the other elements which may also include, in combination, additional elements not listed. This definition adds no new matter and is supported by the specification.

Each of the rejections from the non-final Office Action dated August 5, 2005 is discussed below in connection with the various claims. No new matter has been added. Applicants respectfully request reconsideration of the application in light of the following remarks.

I. INDEPENDENT CLAIMS 1, 41, 50, 72, 90, AND 108

A. Rejections Under 35 U.S.C. § 102(e)

Independent claims 1, 50, 72, 90, and 108 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dutta. With this response, claims 1, 50, 72, 90, and 108 have been amended for clarity and not for reasons relating to patentability. Applicants submit that amended claims 1, 50, 72, 90, and 108 are not anticipated by

Dutta because Dutta fails to disclose all the limitations of amended claims 1, 50, 72, 90, and 108.

Dutta discloses a firewall that controls access. Dutta at col. 2, lns. 3-4. Particularly, Dutta discloses "[t]he access control proxy analyzes the contents of the packet, and identifies an access rule based upon the contents. The action prescribed by the access rule is performed with respect to the packet and any related packets." Dutta at col. 2, lns. 2-6.

Dutta fails to disclose at least "wherein said first action comprises at least storing information related to said first data packet; (f) capturing said second data packet from said network prior to its reception by said source; (g) analyzing a header layer of said second data packet according to a fourth rule; (h) examining, selectively, a dynamically specified portion of said application data layer of said second data packet according to a fifth rule; (i) determining a second action to be taken on said second data packet according to a sixth rule; and (j) performing said second action on said second data packet; and wherein at least one of said fourth rule, said fifth rule, said sixth rule or combinations thereof, is based on said stored information," as claimed in amended claim 1; "a packet analyzer coupled with said memory and operative to analyze said header layer according to a first rule and selectively analyze a dynamically specified portion of said application data layer according to a second rule; and a packet redirector coupled with said memory, said packet analyzer and said routing processor and operative to selectively perform an action on said first packet according to a third rule prior to said conveyance by said routing processor; wherein at least one of said first rule, said second rule, said third rule, or combinations thereof, are based on said stored information," as claimed in amended claim 50; "a packet processor coupled with said router interface and operative to intercept a first packet from a source to a destination, prior to receipt by said router, said packet processor further comprising: a memory operative to store information about a second packet previously transmitted from said destination to said source; a buffer operative to receive and store said first packet for processing; first logic coupled with said buffer and said memory, said first logic operative to apply a first function to a header layer of said first packet and produce a first result; second logic coupled with said buffer and said memory, said second logic operative to apply a second function to a dynamically specified portion of said application data layer of said first packet and produce a second result; and third logic coupled with said buffer, said memory and said first and second logic, said third logic operative to perform an operation on said first packet using a third function and said first and second results; wherein at least one of said first function, said second function, said third function, or combinations thereof, are based on said stored information," as claimed in amended claim 72; "wherein at least one of said first rule, said second rule, said third rule, said first logic, said second logic, said third logic, or combinations thereof, are based on a second packet previously transmitted over said network from said first destination to said first source," as claimed in amended claim 90; or "[a]n edge server coupled between a point-of-presence ("POP") and a network and operative to monitor a bidirectional network traffic stream passing between said POP and said network, said bidirectional network traffic stream comprising a first stream passing from said POP to said network and a second stream passing from said network to said POP, said edge server comprising: a traffic interceptor operative to at least one of selectively intercept said first stream based on at least a portion of said second stream prior to said first stream reaching its intended destination, selectively intercept said second stream based on at least a portion of said first stream prior to said second stream reaching its intended destination, or combinations thereof; and a traffic modifier operative to modify said selectively intercepted stream and reinsert said modified selectively intercepted stream into said network" as claimed in amended claim 108.

Instead, Dutta discloses that "[a]fter the packet is received, an access rule is identified that corresponds to at least one header parameter of the packet." Dutta at col. 2, lns. 35-37. Dutta also discloses, "[t]he access control proxy selects an access rule based upon the contents of the packet. . . . When a packet is referred to an access control proxy process, the proxy process analyzes the contents of the packet and selects an access rule based upon the results the content analysis." Dutta at col. 2, lns. 47-48; col. 4, lns. 59-62. Further, Dutta discloses that after the access rule is selected based on a packet's contents "the access rule is implemented for that packet and *any related packets*." Dutta at col. 2, ln. 66 - col. 3, ln. 1 (emphasis added).

Dutta, however, fails to disclose or suggest that the rule is determined based on bidirectional packet activity, i.e. based on one or more packets traveling in the opposite direction, in terms of the communicating entities, as the present packet under scrutiny. A "related packet," as defined by Dutta, is "another packet in the *same session request* as the first packet." Dutta at col. 3, lns. 1-2 (emphasis added). Dutta further states that "[t]he packet ... will be PASSED or DROPPED in accordance with the selected access rule, as will any other packets *that comprise the connection request*." Dutta at col. 3, lns. 4-8 (emphasis added). While not defined in Dutta, one of ordinary skill in the art would appreciate that a "session" is defined as "a series of interactions between two communication end points that occur during the span of a single connection...." (*See* http://searchwebservices.techtarget.com/sDefinition/0,290660,sid26_gci541649,00.html) Sessions are not necessarily bidirectional. (*See* http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212967,00.html) Further, one of ordinary skill in the art would appreciate that a "session request" or a "connection request" is the one or more packets sent unidirectionally from the requestor to requestee to initiate the session. (*See* Dutta, Col. 1, lns. 50-58. *See Also* http://www22.verizon.com/about/community/learningcenter/articles/displayarticle1/0,1727,1150z1,00.html) This is distinguished from a session acknowledgment which is the response, sent from the requestee back to the requestor to acknowledge receipt of the request. Accordingly, one of skill in the art would not conclude, and Dutta fails to suggest, that a session request further includes a session acknowledgement or other packets flowing in the other direction from the requestee to the requestor. Therefore, Applicants submit that, Dutta fails to disclose or suggest rule application based on bidirectional packet analysis as claimed by Applicants.

Furthermore, it would not be obvious to one skilled in the art to add the missing limitations to the system disclosed by Dutta because the system of Dutta is directed to access control, i.e. to determining whether to pass or drop a given packet based on an analysis of the entire packet, rather than only the packet header. Thus, to determine whether or not to drop a packet sent from a sender to a host, Dutta examines the payload of the packet in order to determine the "ultimate target" of the request. Dutta at col. 1, lns. 48-58. Furthermore, Dutta works towards this ultimate goal by analyzing packets that are a part of the same session/connection request, as a session request may actually be spread over multiple packets sent from the requestor. *See* Dutta at col. 3, lns. 1-2. As soon as a packet or set of packets of a session/connection request containing sufficient payload information to determine an access rule have been analyzed, the remaining packets of that request are processed according to the same access rule. Dutta, Col. 3, lns. 4-8. As discussed above, Dutta's disclosure of the same session request necessarily means that system of Dutta, as disclosed, performs only unidirectional packet analysis. Moreover, because Dutta functions without the added limitations; adding the missing limitations would fail to add any benefit to Dutta being able to determine the "ultimate target of . . . a connection request from a sender to a destination host," for the purposes of determining whether or not to pass or drop a given packet. (Dutta, at col. 1, lns. 48-49), since all of the information needed to complete the analysis disclosed by Dutta is contained within the one or more packets of the connection request. Adding bidirectional packet analysis in order to determine rules to be applied to packets would only result in a less efficient system since more work would have be done to store the information despite the fact that the information would never be utilized by the system of Dutta to determine whether to pass or drop a packet. Such inefficiency is contrary to Dutta's goal. *See* Dutta at col. 6, ln. 31. Thus, it would not be obvious for one of ordinary skill in the art to add the limitations missing from Dutta.

Accordingly, because Dutta fails to disclose all the limitations of amended claims 1, 50, 72, 90, and 108, Applicants respectfully request that the Examiner withdraw the rejection of these claims.

B. Rejections Under 35 U.S.C. § 103(a)

Independent claim 41 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Dutta in view of Kloth. With this response, claim 41 has been amended for clarity and not for reasons relating to patentability. As discussed above, Dutta fails to disclose bidirectional packet analysis, as claimed in amended claim 41: "wherein at least one of said first rule, said second rule, said third rule, said fourth rule, said fifth rule, said sixth rule, said seventh rule, or combinations thereof, are based on a second packet previously transmitted over said network from said first recipient to said source."

Kloth also fails to disclose or suggest this limitation. Kloth discloses "[an] apparatus and method that provides a routing engine for processing data packets based upon certain rules that are compiled and applied real-time via a just-in-time (JIT) compiler, a runtime compiler, or the like." Kloth at Abstract.

Instead of disclosing all of the limitations in amended claim 41, Kloth discloses, "[a] way to classify the packet as early as possible with as much information as possible—from all OSI Layers and from all the rules—to be applied to every IP packet. The present system does not perform the classification sequentially, but instead performs it in full (for the entire IP flow), as early as possible in the process. . . . The routing engine will receive and parse an incoming IP flow. For the outset, the engine looks at (or analyzes) all parts of the IP flow, for instance the IP header, TCP header, Application header, etc. The engine then decides whether to forward or buffer the data packet. A set of rules are used to define a pattern (or set of patterns) to be analyzed (or compared matched) in the incoming IP data flow. . . . Upon detection of a certain pattern, actions can be performed upon the IP flow and or individual IP packets." Kloth col. 4, lns. 27-54.

Kloth's goal is to find patterns in an IP stream. Kloth at col. 2, lns. 40-46 ("[t]he configuration should utilize a set of rules for routing the various packets within an IP stream according to patterns along any point within the IP stream. . . . The system should analyze entire IP flows (or packets) for such patterns"); col. 6, lns. 13-

18 ("[t]he present invention analyzes . . . all available information"); col. 10, lns. 17-20 ("[t]he present invention provides for looking at every part of a packet").

To find patterns, Kloth only discloses unidirectional packet analysis: "[a] set of rules are used to define a pattern (or set of patterns) to be analyzed (or compared/matched) in the incoming IP data flow;" (Kloth at col. 4, lns. 44-46); "an intruder to a system might be detected, via pattern comparisons and the like established as a function of certain rules. The intruder will have a certain IP address. The intruder's IP stream (or packets) are discarded;" (Kloth at col. 10, lns. 34-38); "[t]raffic flow from 'spammers' might also be eliminated by detecting the source address pattern of machines sending such undesired information, and thereafter dropping any packets from that source address;" (Kloth at col. 10, lns. 43-46). Here, Kloth's use of the terms "IP stream" and "traffic flow" is directed to a unidirectional stream/flow since the intruder's/spammer's packets could not be discarded if they already traveled from the destination to the source since they would have already passed the packet analyzer. Furthermore, Kloth explicitly states that the disclosed system is detecting the "source addresses" as opposed to destination to source information. *See* Kloth at col. 10, lns. 43-46. Thus, one of ordinary skill in the art would appreciate that packet analysis, as disclosed in Kloth, must be occurring in a single direction so as to be able to detect the source address and to be able to discard the intruder's IP stream by analyzing the "incoming IP data flow." Consequently, "incoming IP data flow" must also mean the IP flow that is part of the IP stream traveling in a single direction. Therefore, Kloth, alone or in combination with Dutta, fails to disclose bidirectional packet analysis of Applicant's claims.

In addition, it would not be obvious to one skilled in the art to add the missing limitation to Kloth. Kloth fails to disclose how it determines if it found a pattern, other than stating that it reviews the incoming IP flow and that "[t]he patterns to be detected are determined essentially by the formulated rules." Kloth at col. 4, lns. 44-46; col. 9, lns. 65-67. Kloth gives no indication that pattern identification would be improved by reviewing anything other than the incoming IP flow, especially in light of Kloth's disclosure that it examines the incoming IP flow to perform pattern analysis when acting like a router or firewall device. *See* Kloth at col. 4, lns. 39-40; col. 10, lns. 34-38.

When acting like a router, Kloth "receive[s] and parse[s] an incoming IP flow." Kloth at col. 4, lns. 40-41. Thus, under Kloth, no advantage would be gained in performing bidirectional packet analysis in order to determine to where a packet should be routed. Furthermore, when acting as a firewall, Kloth discloses that "an intruder to a system might be detected, via pattern comparisons and the like established as a function of certain rules. The intruder will have a certain IP address. The intruder's IP stream (or packets) are discarded." Kloth at col. 10, lns. 34-38. Thus, adding bidirectional packet analysis would in no way assist in determining whether a packet came from a suspect IP address.

Kloth and Dutta each fail to disclose all of the limitations of amended claim 41 and, as discussed above, it would not be obvious to one skilled in the art to add the missing limitations to either reference. Accordingly, because Dutta in view of Kloth fail to disclose all the limitations of amended claim 41, Applicants respectfully request that the Examiner withdraw the rejections of these claims.

II. Dependent Claims 2-40, 42-49, 51-71, 73-89, 91-107, and 109-111

Dependent claims 2-25, 29-40, 51-62, 64-71, 73-85, 87-89, 91-99, ~~102~~101-103, 105-107, and 109-111 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dutta. Dependent claims 26-28, 42-49, 63, 86, 100, and 104 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Dutta in view of Kloth. With this response, claims 2, 67 and 111 have been cancelled.

As explained above, Dutta and Kloth fail to disclose all the limitations of amended claims 1, 41, 50, 72, 90, and 108; therefore, the cited references fail to disclose all the limitations of those claims that depend on amended claims 1, 41, 50, 72, 90, and 108. Accordingly, Applicants respectfully request that the Examiner withdraw the rejections of these claims.

CONCLUSION

In view of the foregoing remarks, Applicants submit that the pending claims are in condition for allowance. Applicants respectfully request reconsideration of the application. If there are any questions concerning this response, the Examiner is invited to phone the undersigned attorney at (312) 321-4200.

Respectfully submitted,

Dated: 10-19-05

Andrea Lynn Evensen
Registration No. 56,531
Attorney for Applicants

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200